

Unit 3- Internet Security and Privacy

Internet security overview.

Internet security consists of a range of security strategy for protecting activities and transactions conducted online over the internet. These strategies are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cyber security and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

In today's world, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online. This means that tons of data and sensitive information are constantly being shared over the internet. The internet is mostly private and secure, but it can also be an insecure channel for exchanging information. With a high risk of interference by hackers and cybercriminals, internet security is a top priority for individuals and businesses alike.

Any Internet security Technique can be supporting the following principles:

1. **Confidentiality:** Data is kept protected against threats and unauthorized access.
2. **Integrity:** Data is kept accurate and reliable by preventing accidental or intentional alterations or deletion.
3. **Availability:** Data is kept accessible to those who are authorized to have access.

Advantages Internet Security:

- 1) Protects system against viruses, worms, spyware and other unwanted programs.
- 2) Protection against data from theft.
- 3) Protects the computer from being hacked.
- 4) Minimizes computer freezing and crashes.

5) Gives privacy to users

Types of internet security threats:-

- 1) **Malware:** Short for "malicious software," malware comes in several forms, including computer viruses, worms, Trojans, and dishonest spyware.
- 2) **Credit card fraud:** It is an inclusive term for fraud committed using a payment card, such as a credit card or debit card.^[1] The purpose may be to obtain goods or services, or to make payment to another account which is controlled by a criminal.
- 3) **Spam:** Spam refers to unwanted messages in your email inbox. In some cases, spam can simply include junk mail that advertises goods or services you aren't interested in. These are usually considered harmless, but some can include links that will install malicious software on your computer if they're clicked on.
- 4) **Spoofing:** Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or IP address.
- 5) **Internet hour theft:** Internet hour theft refers to the theft in a manner where the unauthorized person uses internet hours paid by another person. The unauthorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

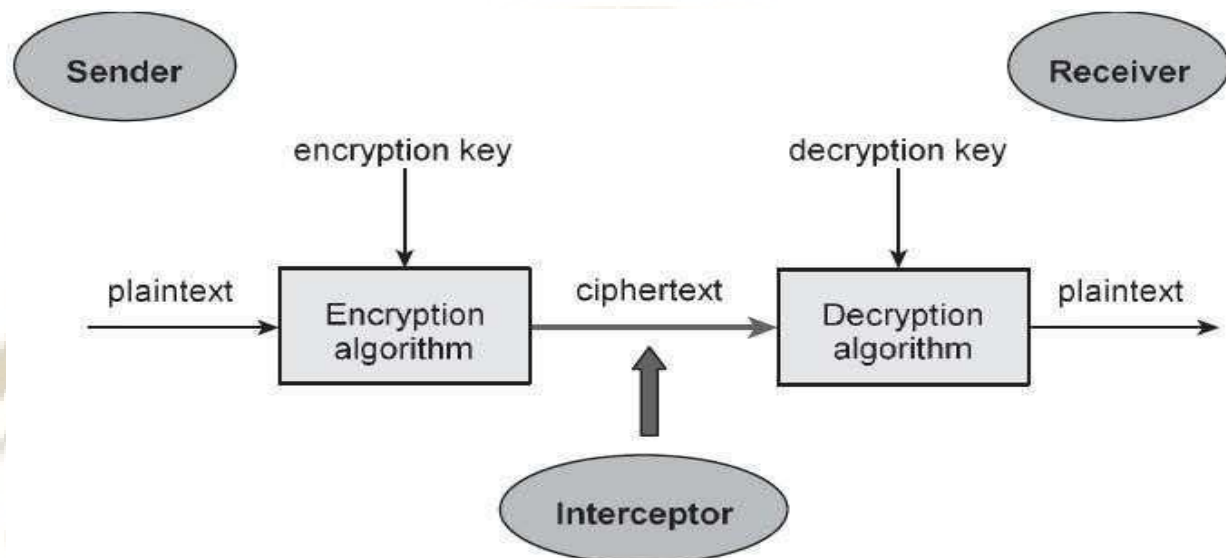
Data Encryption

Data Encryption (Definition):- Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext.

Cryptosystem:- A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.

Unit-3 Internet Security and Privacy

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below :-



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows –

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

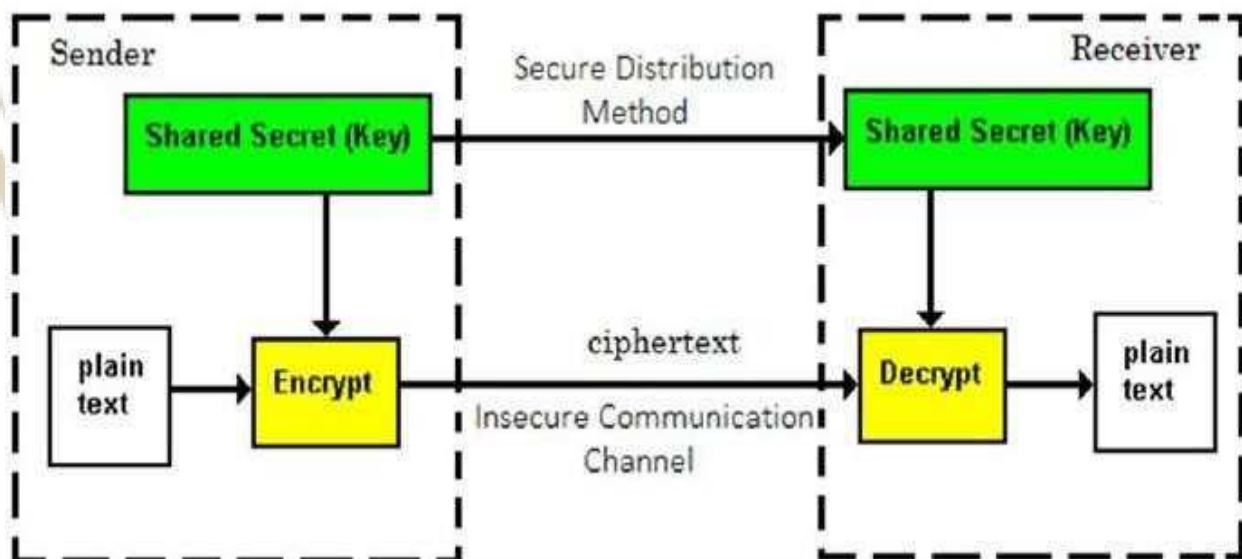
- **Decryption Algorithm**, It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key**. It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key**. It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

Symmetric Key Encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems.

A few well-known examples of symmetric key encryption methods are – Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Unit-3 Internet Security and Privacy

Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are –

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is $n \times (n - 1)/2$.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

There are two restrictive challenges of employing symmetric key cryptography.

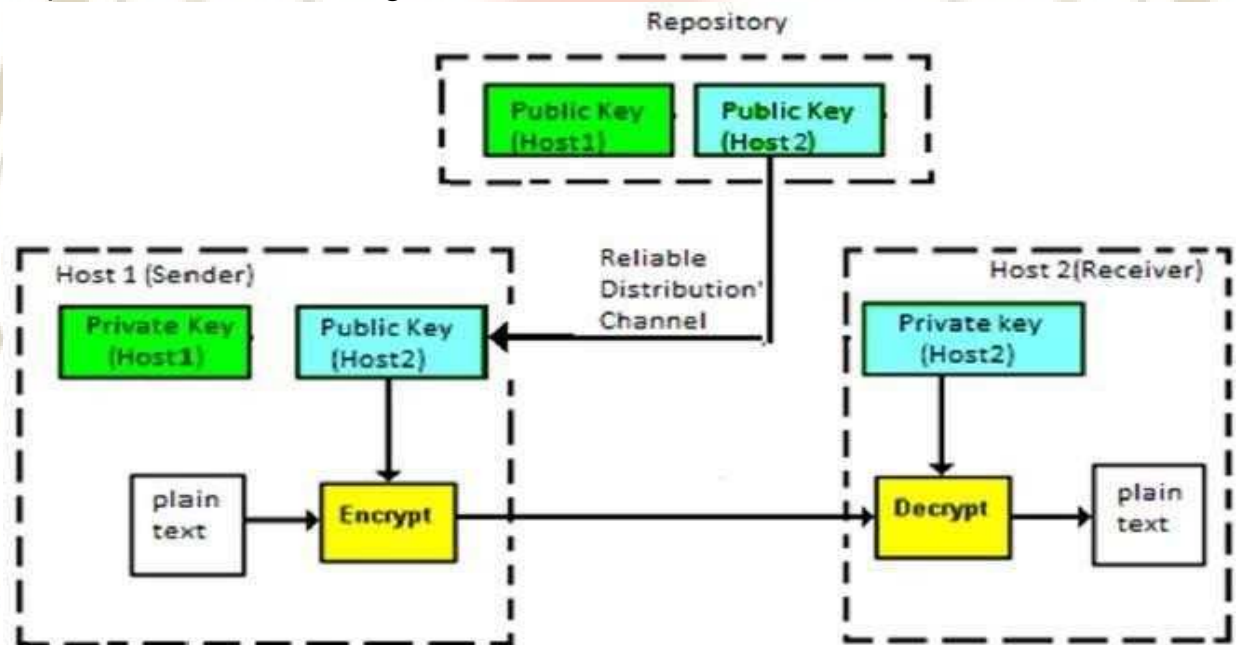
- **Key establishment** – Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** – Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between

online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Public Key Encryption/ Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration –



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows –

- Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.

Unit-3 Internet Security and Privacy

- When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits.
- Host2 uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

You may think, how can the encryption key and the decryption key are 'related', and yet it is impossible to determine the decryption key from the encryption key? The answer lies in the mathematical concepts. It is possible to design a cryptosystem whose keys have this property. The concept of public-key cryptography is relatively new. There are fewer public-key algorithms known than symmetric algorithms.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge – the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process – that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

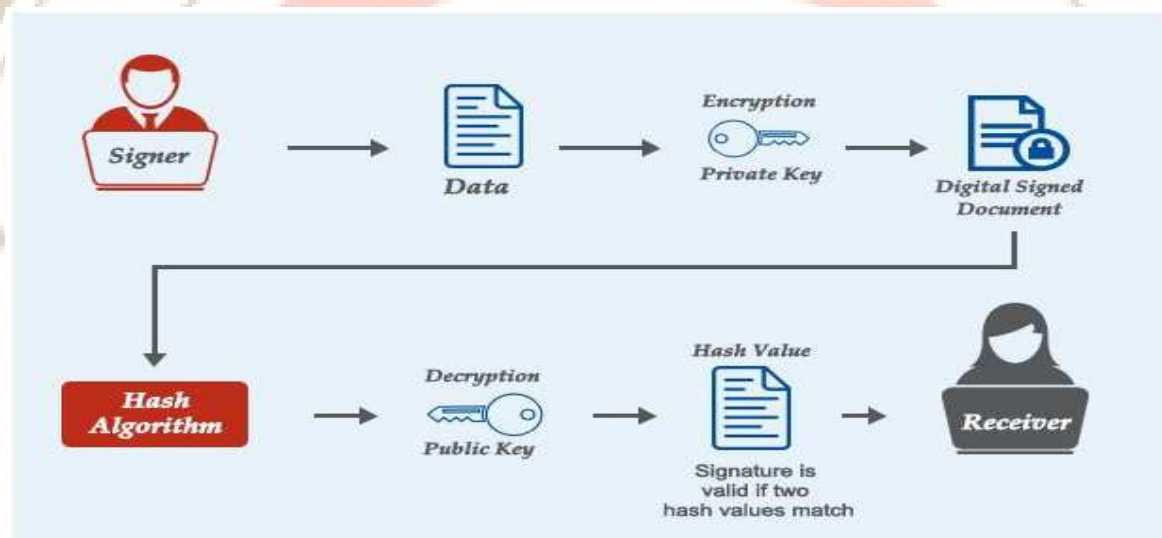
Concepts of Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it

offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Working of Digital signature:

Digital signatures are based on Public Key infrastructure. By this mechanism, two keys are generated, a **Public Key** and **Private Key**. The private key is kept by the signer and it should be kept securely. On the other hand, the receiver must have the public key to decrypt the message. For example, a person named Bob wants to send an encrypted message to Alice. As stated above, Bob must have a private key to sign the message digitally.



Before encrypting the message using the private key, an algorithm named 'MD algorithm' encrypts the message to be sent by Bob into a 128/256-bit format known as a **hash value**. Then Bob's private key encrypts this hash value. On completion of both the processes, Bob's message is said to be digitally signed.

On the side of Alice, the digitally signed message is decrypted with the help of the signer's public key. The public key decrypts the message and converts it into another hash value. Then the program which is used to open the message (e.g., MS Word, Adobe Reader etc.) compares this hash value to the original hash value which was generated on Bob's side. If the hash value on Alice's side matches with the hash value generated on Bob's side, then the program will allow the message to open up and displays the message "The document has not been modified since this signature was

applied.” The program will not allow the document to open if both the hash values don’t match.

Benefits of digital signatures:-

Security is the main benefit of digital signatures. Security capabilities embedded in digital signatures ensure a document is not altered and signatures are legitimate. Security features and methods used in digital signatures include the following:

- **Personal identification numbers (PINs), passwords and codes.** Used to authenticate and verify a signer's identity and approve their signature. Email, username and password are the most common methods used.
- **Asymmetric cryptography.** Employs a public key algorithm that includes private and public key encryption and authentication.
- **Checksum.** A long string of letters and numbers that represents the sum of the correct digits in a piece of digital data, against which comparisons can be made to detect errors or changes. A checksum acts as a data fingerprint.
- **Cyclic redundancy check (CRC).** An error-detecting code and verification feature used in digital networks and storage devices to detect changes to raw data.
- **Certificate authority (CA) validation.** CAs issue digital signatures and act as trusted third parties by accepting, authenticating, issuing and maintaining digital certificates. The use of CAs helps avoid the creation of fake digital certificates.
- **Trust service provider (TSP) validation.** A TSP is a person or legal entity that performs validation of a digital signature on a company's behalf and offers signature validation reports.

Concepts about Firewall Security

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined

Unit-3 Internet Security and Privacy

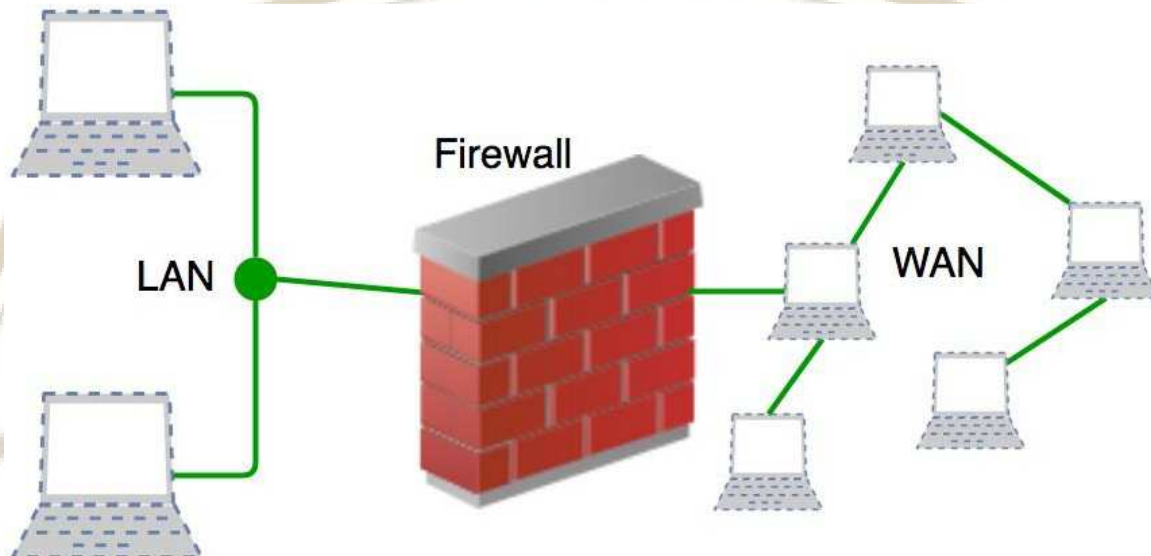
set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic

Reject : block the traffic but reply with an “unreachable error”

Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.



How Firewall Works

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy.

Unit-3 Internet Security and Privacy

Default policy only consists of action (accept, reject or drop). Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to *accept*, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as *drop* (or reject) is always a good practice.

Generation of Firewall

Firewalls can be categorized based on its generation.

1. **First Generation- Packet Filtering Firewall** : Packet filtering firewall is used to control network access by monitoring outgoing and incoming packet and allowing them to pass or stop based on source and destination IP address, protocols and ports. It analyses traffic at the transport protocol layer (but mainly uses first 3 layers). Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.
2. Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

3. **Second Generation- Stateful Inspection Firewall** : Stateful firewalls (performs Stateful Packet Inspection) are able to determine the connection state of packet, unlike Packet filtering firewall, which makes it more efficient. It keeps track of the state of networks connection travelling across it, such as TCP streams. So the filtering decisions would not only be based on defined rules, but also on packet's history in the state table.

4. **Third Generation- Application Layer Firewall** : Application layer firewall can inspect and filter the packets on any OSI layer, up to the application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused.

In other words, Application layer firewalls are hosts that run proxy servers. A proxy firewall prevents the direct connection between either side of the firewall, each packet has to pass through the proxy. It can allow or block the traffic based on predefined rules.

Note: Application layer firewalls can also be used as Network Address Translator(NAT).

5. **Next Generation Firewalls (NGFW)** : Next Generation Firewalls are being deployed these days to stop modern security breaches like advance malware attacks and application-layer attacks. NGFW consists of Deep Packet Inspection, Application Inspection, SSL/SSH inspection and many functionalities to protect the network from these modern threats.